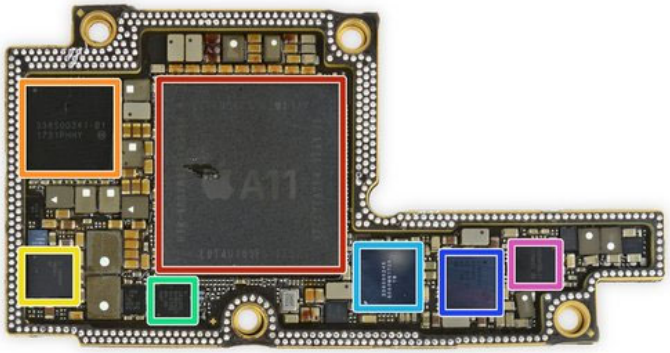
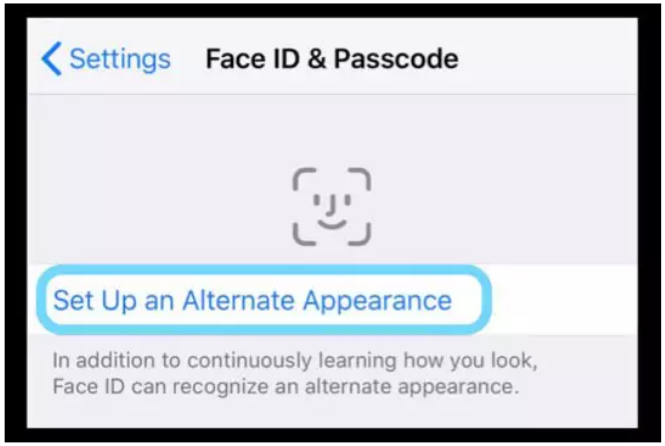
EXHIBIT H

Claim Chart for U.S. Patent No. 9,665,705 ("the '705 Patent")

The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhone type cellular phones and Apple iPad type tablets, including the Apple iPhone X and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the '705 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the '705 Patent literally and, to the extent not literally, under the doctrine of equivalents.

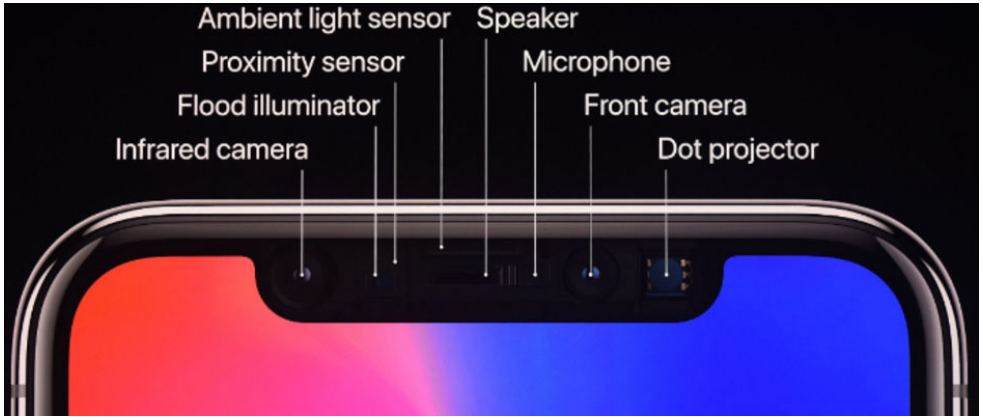
Claim 1	Apple iPhone X
1. A system for providing secure access to a controlled item, the system comprising:	To the extent that the preamble is deemed to be a limitation, the Apple iPhone X is configured to use a system in accordance with this claim.
1a. a memory comprising a database of biometric signatures;	**The Apple iPhone X includes a memory comprising a database of biometric signatures.** More specifically, the Apple iPhone X has a secure enclave in the A11 chip. For Face ID, the user's face image is translated into encrypted mathematical data and stored in the secure enclave. The stored mathematical data of face image is compared with a face image received by the sensor to allow or deny access to the device. Face ID data, including mathematical representations of your face, is encrypted and only available to the Secure Enclave. This data never leaves the device. It is not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of your face calculated during enrollment. • The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching. Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf

Claim 1	Apple iPhone X
	 • Apple APL1W72 A11 Bionic SoC layered over SK Hynix H9HKNNNDBMAUUR 3 GB LPDDR4x RAM https://www.ifixit.com/Teardown/iPhone+X+Teardown/98975

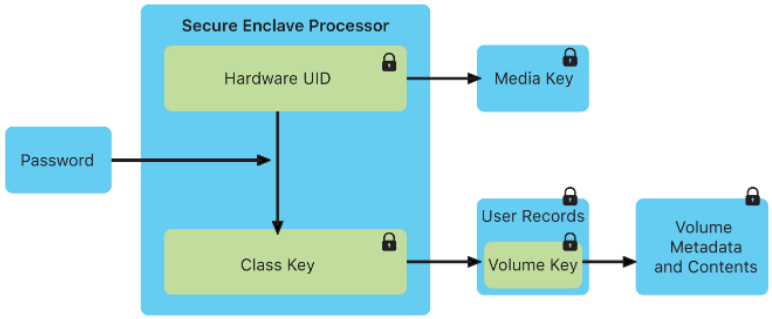
Claim 1	Apple iPhone X
	How-To Add Multiple Users to Face ID If you want to add a new user to Face ID on your iPhone, the steps are pretty straightforward. **Here is what you will need to do:** 1. Open **Settings** 2. Scroll and select **Face ID & Passcode** 3. Enter Passcode 4. Tap **Set up an Alternative Appearance**  https://appletoolbox.com/multiple-face-id-users-ios-12/

Claim 1	**Apple iPhone X**
	 https://support.apple.com/guide/iphone/set-up-face-id-iph6d162927a/ios

Claim 1	**Apple iPhone X**
1b. a transmitter sub-system comprising:	As set forth in elements 1b1, 1b2, and 1b3 below, the Apple iPhone X includes a transmitter subsystem.
1b1. a biometric sensor configured to receive a biometric signal;	**The Apple iPhone X includes a biometric sensor configured to receive a biometric signal.** More specifically, the Apple iPhone X's Face ID uses a camera system, called the TrueDepth camera system, which includes an image sensor. The image sensor is used to capture a detailed depth map of the user's facial features for Face ID. With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf The TrueDepth camera is intelligently activated; for example, by tapping to wake your screen, from an incoming notification that wakes the screen, or by raising to wake your iPhone. Each time you unlock your device, the TrueDepth camera recognizes you by capturing accurate depth data and an infrared image. This information is matched against the stored mathematical representation to authenticate. https://support.apple.com/en-us/HT208108 "Camera includes image sensor. Image sensor may be, for example, an array of sensors. Sensors in the sensor array may include, but not be limited to, charge coupled device (CCD) and/or complementary metal oxide semiconductor (CMOS) sensor elements to capture infrared images (IR) or other non-visible electromagnetic radiation." the '835 Publication, ¶ ¶043 "Image sensor is an IR image sensor and the image sensor is used to capture infrared images used for face detection, facial recognition authentication, and/or depth detection." the '835 Publication, ¶ ¶044

Claim 1	**Apple iPhone X**
	 https://www.ifixit.com/Teardown/iPhone+X+Teardown/98975  https://www.phonearena.com/news/TrueDepth-camera-iPhone-X-Face-ID-Animoji_id108355

Claim 1	Apple iPhone X
1b2. a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and	**The Apple iPhone X includes a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute.** More specifically, the Apple iPhone X includes a secure enclave processor (SEP) that matches a face image against the enrolled facial image data and generate a matching score. The matching score generated by SEP is then transmitted to a processor. When the matching score is above the unlock threshold, the device can be unlocked. Facial matching is performed within the secure enclave using neural networks trained specifically for that purpose. We developed the facial matching neural networks using over a billion images, including IR and depth images collected in studies conducted with the participants' informed consent. We worked with participants from around the world to include a representative group of people accounting for gender, age, ethnicity, and other factors. We augmented the studies as needed to provide a high degree of accuracy for a diverse range of users. Face ID is designed to work with hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it's designed to work indoors, outdoors, and even in total darkness. An additional neural network that's trained to spot and resist spoofing defends against attempts to unlock your phone with photos or masks. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf a device-specific random pattern. A portion of the A11 Bionic processor's neural engine—protected within the Secure Enclave—transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of your face captured across a variety of poses. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf

Claim 1	Apple iPhone X
1b3. a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and	**The Apple iPhone X includes a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute.** More specifically, the iPhone X includes a secure enclave processor (SEP) configured to deliver secure access signal to application processors. The Secure Enclave also maintains the integrity of its cryptographic operations even if the device kernel has been compromised. Communication between the Secure Enclave and the application processor is tightly controlled by isolating it to an interrupt-driven mailbox and shared memory data buffers.  The Secure Enclave processor. https://support.apple.com/guide/security/secure-enclave-overview-sec59b0b31ff/web

Claim 1	**Apple iPhone X**
1c. a receiver sub-system comprising:	As set forth in elements 1c1 and 1c2 below, the Apple iPhone X includes a receiver sub-system.
1c1. a receiver sub-system controller configured to: receive the transmitted secure access signal; and	**The Apple iPhone X includes receiver sub-system configured to receive the transmitted secure access signal.** More specifically, the iPhone X includes a processor that utilizes a secured channel to receive encrypted secure biometric data from a secure enclave processor (SEP). Face ID data, including mathematical representations of your face, is encrypted and only available to the Secure Enclave. This data never leaves the device. It is not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of your face calculated during enrollment. • The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching. Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf
1c2. provide conditional access to the controlled item dependent upon said information;	**The Apple iPhone X includes receiver sub-system configured to provide conditional access to the controlled item dependent upon said information.** More specifically, the iPhone X includes a processor that controls the unlocking of the phone based on the matching score received from a secure enclave processor (SEP).

Claim 1	Apple iPhone X
	Facial matching is performed within the secure enclave using neural networks trained specifically for that purpose. We developed the facial matching neural networks using over a billion images, including IR and depth images collected in studies conducted with the participants' informed consent. We worked with participants from around the world to include a representative group of people accounting for gender, age, ethnicity, and other factors. We augmented the studies as needed to provide a high degree of accuracy for a diverse range of users. Face ID is designed to work with hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it's designed to work indoors, outdoors, and even in total darkness. An additional neural network that's trained to spot and resist spoofing defends against attempts to unlock your phone with photos or masks. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf a device-specific random pattern. A portion of the A11 Bionic processor's neural engine—protected within the Secure Enclave—transforms this data into a mathematical representation and compares that representation to the enrolled facial data. This enrolled facial data is itself a mathematical representation of your face captured across a variety of poses. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf

Claim 1	**Apple iPhone X**
1d. wherein the transmitter sub-system controller is further configured to:	The Apple iPhone X includes a transmitter sub-system controller that is configured to be used as set forth in elements 1d1, 1d2, and 1d3 below.
1d1. receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry;	**The Apple iPhone X includes transmitter sub-system controller configured to receive a series of entries of the biometric signal, said series being characterized according to at least one of the number of said entries and a duration of each said entry.** More specifically, the Apple iPhone X receives a series of face images through its image sensor on the TrueDepth camera system by having users move or tilt their head to set up a Face ID.  https://support.apple.com/en-us/HT208109

Claim 1	**Apple iPhone X**
	 https://www.ifixit.com/Teardown/iPhone+X+Teardown/98975
1d2. map said series into an instruction; and	**The Apple iPhone X includes transmitter sub-system controller configured to map said series into an instruction.** More specifically, the Apple iPhone X includes a secure enclave processor (SEP) that can map biometric signals into an instruction.

Claim 1	Apple iPhone X
	Face ID data, including mathematical representations of your face, is encrypted and only available to the Secure Enclave. This data never leaves the device. It is not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of your face calculated during enrollment. • The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching. Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf
1d3. populate the database according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.	**The Apple iPhone X includes transmitter sub-system controller configured to populate the data base according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device** More specifically, the Apple iPhone X includes a secure enclave processor (SEP) that can generate an authentication score based on its program instructions to determine whether the device can be unlocked.

Claim 1	Apple iPhone X
	Face ID data, including mathematical representations of your face, is encrypted and only available to the Secure Enclave. This data never leaves the device. It is not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of your face calculated during enrollment. • The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching. Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf